8Ш

УДК 004.415.24

И.В. Швидченко
Институт кибернетики имени В.М. Глушкова НАН Украины, г. Киев
sh_inet@rambler.ru

Методы стеганоанализа для графических файлов

Статья посвящена проблеме выявления стеганографического скрытия в файлах форматов BMP и JPEG. Проводится анализ различных известных стеганоаналитических методов. Приводится их классификация и краткий обзор. Для установления факта присутствия в контейнере скрытой информации предлагается последовательное применение представленных методов.

Введение

Развитие компьютерных методов обработки информации позволило существенно повысить уровень обеспечения информационной безопасности [1]. Значительных успехов в этом направлении удалось добиться с использованием современных криптографических методов. Однако в целом ряде задач информационной безопасности их становится недостаточно, поскольку они не позволяют скрыть сам факт наличия или передачи информации. Решать подобные проблемы стало возможным с использованием стеганографических методов защиты информации.

Наряду с созданием новых стеганографических алгоритмов скрытия информации не менее актуальной является разработка методов современного стеганоанализа.

Основная задача стеганоанализа – установление факта присутствия в контейнере скрытой информации. В ходе решения данной задачи стеганоаналитиком используются различные методы анализа. Однако при попытке автоматизации процесса на множестве контейнеров возникает проблема выбора метода анализа, поскольку реализации различных методов могут давать противоречивые результаты, что обусловлено, в первую очередь, неравенством вероятностей возникновения ошибок распознавания для этих реализаций. Кроме того, в условиях априорной неопределённости относительно типа стеганосистемы значительную сложность представляет вопрос выбора исходных данных для анализа. Снижение объёма анализируемых данных потенциального контейнера ведёт к увеличению вероятности возникновения ошибки первого рода (вероятность обнаружения скрытого сообщения в пустом контейнере), что, в свою очередь, увеличивает вероятность возникновения ошибок второго рода (вероятность принятия заполненного контейнера за пустой). Изменение правил выборки анализируемых данных ведет к возрастанию ошибок распознавания.

Таким образом, в настоящее время для решения задачи стеганоанализа и последующего извлечения скрытой информации необходим комплексный подход, позволяющий выделить на множестве результатов те из них, которые способствуют минимизации вероятности ошибки второго рода при заданном уровне вероятности ошибки первого рода.

Практическая стойкость стеганосистем. Методы стеганоанализа контейнеров-изображений

Самым распространенным на сегодня методом стеганографического скрытия является метод замены наименее значимых бит [2]. Идея метода заключается в замене от одного до четырех младших битов в байтах цветового представления точек исходного изображения битами скрываемого сообщения. Возможность такой замены обусловлена наличием в изображениях структурной избыточности. Метод применяется к растровым изображениям, представленным в формате без компрессии. Одним из таких форматов выступает BMP. Положительной стороной BMP является высокое качество изображения, а также простота формата, что делает его популярным для применения в качестве контейнера.

Еще один метод стеганографического преобразования информации основан на использовании особенностей файлов, сжатых с потерей данных. Популярным графическим форматом, использующим алгоритм сжатия данных с потерями, является JPEG. При скрытии в JPEG-файлы информация прячется не в значения цветовых составляющих отдельных пикселов, а в биты квантованных дискретных косинусных коэффициентов. С позиции стеганографии файлы данного формата позволяют скрывать сравнительно большие объемы информации.

Безопасность стеганосистем, использующих тот или иной метод стеганографического скрытия, описывается и оценивается их стойкостью. Оценить стойкость стеганосистемы в теоретико-информационном смысле [3] на практике невозможно, поэтому вводится понятие стеганографической стойкости в практическом смысле.

Стеганографическая система называется *стойкой в практическом смысле*, если не существует стеганоаналитического алгоритма, который был бы способен обнаружить наличие скрытой информации [4].

Проведенный анализ существующих методов стеганоанализа показал, что в зависимости от *используемых исходных данных* их можно разделить на две основные группы:

1. Методы, предназначенные для работы с конкретными заранее известными стеганографическими алгоритмами.

2. Методы, предназначенные для любых алгоритмов стеганографии. Стеганоанализ данными методами не требует знания использованного стеганографического алгоритма, алгоритма шифрования, сжатия, ключа и длины сообщения. Известные методы этой группы обычно построены на алгоритмах, требующих предварительного «обучения» на сериях из заполненных и пустых контейнеров.

Методы обеих групп построены с учетом предположения о недоступности исходного пустого контейнера, который был использован для внедрения информации в исследуемый стеганоконтейнер.

К первой группе относят *сигнатурные* и *схемные* методы анализа.

Суть **сигнатурных методов** заключается в синтаксическом анализе предъявленной на вход распознающего устройства последовательности терминальных символов, определяющих контейнер. В случае обнаружения принадлежности предъявленной на вход распознавателя цепочки терминальных символов языку, описывающему ту или иную стеганосистему, принимается решение об ее использовании для скрытия информации. В качестве терминальных символов обычно берут все или часть стандартных символов ASCII – латинские буквы, цифры и специальные символы.

К достоинствам этих методов относится возможность получения результата, который однозначно характеризует примененную для сокрытия данных стеганосистему. Основным недостатком является небольшое (менее 10%) число стеганопрограмм, оставляющих в контейнерах свои сигнатуры [5].

Схемные методы применяются для проверки гипотез о наличии стеганографического вложения с априорно *известной* стеганосистемой. В работе [6] приведено описание применения статистического метода Хи-квадрат для проверки гипотезы о наличии данных, скрытых стеганопрограммами Jsteg, Jpeg Hide&Seek и OutGuess. При этом используются знания о распределении статистики по данным контейнеров, которые характерны именно для результатов работы указанных программ.

Достоинством методов данного класса является относительно низкая вероятность возникновения ошибок, а также тот факт, что по положительному результату анализа аналитик идентифицирует стеганосистему, не оставляющую «следов» (сигнатур) в контейнере, что позволяет предпринять попытку извлечения скрытой информации.

Во вторую группу входят *визуальные* и *статистические* методы.

Визуальные методы базируются на способности зрительной системы человека анализировать зрительные образы и выявлять существенные различия в сопоставляемых изображениях.

Метод визуального анализа является самым простым способом анализа графических файлов, поскольку для этого достаточно просто посмотреть на перехваченное изображение. Тем не менее, этот метод анализа уже способен установить некоторые ограничения на объем скрываемых данных. Так, для полноцветных реалистичных изображений в формате BMP незаметными для человеческого глаза будут искажения менее 3% [7], [8]. В случае с JPEG визуально определить присутствие скрытой информации невозможно. Если в результате скрытия в изображении возникают незначительные искажения, то их можно объяснить применением процедуры сжатия.

Метод визуального анализа битовых срезов. Основная идея метода заключается в сравнении изображения в целом с изображениями его битовых срезов [9]. С помощью программы изображение просматривают по слоям – битовым срезам. Учитывая то, что интенсивность каждого цвета определяется ровно одним байтом, всего необходимо просмотреть 8 таких срезов. Для каждого из трех цветов первый срез – это изображение, построенное самыми младшими битами, второй срез – изображение, построенное вторыми битами и т.д. Полученное изображение битового среза просматривают и визуально сравнивают с анализируемым изображением.

Для метода визуального анализа битовых срезов большое значение имеет то, как именно осуществляется запись скрываемой информации. Если она записывается в подряд идущие биты или равномерно распределяет биты сообщения (на основе генератора псевдослучайных чисел) по всему изображению, то факт скрытия может быть установлен с большой вероятностью. Также визуально можно определить наличие встроенной информации в случае записи сообщения с заполнением. Поскольку вероятностные характеристики сообщения не совпадают с вероятностными характеристиками младших бит пустого контейнера, то при просмотре битового среза со встроенными данными будет отчетливо видна граница между заполненной и не тронутой частью. Для того чтобы вероятностные характеристики совпадали, при записи информации с заполнением, сообщение необходимо зашифровывать [10].

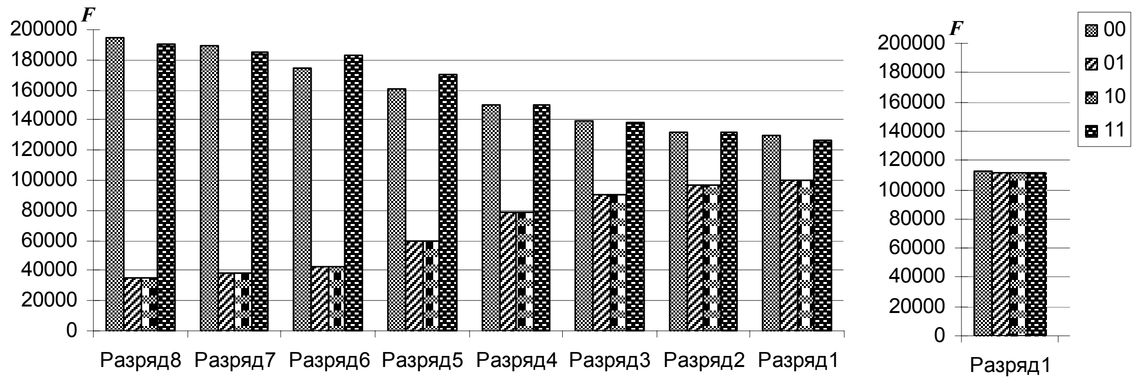
В случае с JPEG-файлами данный метод анализа малопригоден, так как изменение любого коэффициента преобразования приводит к изменению множества пикселов изображения. Внедрение сообщения в младшие биты дискретных косинусных коэффициентов незначительно изменит каждый из 256 пикселов, что визуально незаметно [11].

Статистические методы базируются на понятии «естественного» контейнера. Суть методов заключается в оценивании вероятности существования стеганографического вложения с *неизвестной* стеганосистемой на основе критерия оценки близости исследуемого контейнера к «естественному».

К достоинствам этой группы методов относится неограниченная область применения, что довольно существенно как при проверке гипотезы о наличии стеганографического вложения с неизвестной стеганосистемой, так и при разработке схемных методов стеганоанализа. Основным недостатком методов этого класса является само предположение о существовании «естественного» контейнера. Рассмотрим ряд статистических методов, применяемых на практике.

Метод оценки числа переходов значений младших бит в соседних элементах изображения. В методе используется знание, что между младшими битами соседних элементов и между ними и остальными битами естественных контейнеров имеются корреляционные связи. При анализе графических файлов формата BMP в качестве элементов анализируемой последовательности выбираются *наименее значащие биты цветовых составляющих* рядом стоящих пикселов изображения. При исследовании файлов формата JPEG – *младшие биты соседних дискретных косинусных коэффициентов*, отличных от 0 и 1.

Зависимость между битами в соответствующих разрядах элементов контейнера имеет марковский характер [12]. При этом параметры зависимости определяются номером разряда. Под «переходом» понимают переход значения i-го элемента последовательности в значение $i+1$ элемента последовательности x, $i = 1,2,...,n-1$, n – длина последовательности. Так как последовательности являются двоичными, то анализируется четыре вида переходов: из 0 в 0, из 0 в 1, из 1 в 0 и из 1 в 1. По полученным результатам строится гистограмма. Для каждого разряда первый столбец гистограммы показывает число переходов в потоке НЗБ из 0 в 0, второй столбец – из 0 в 1, третий столбец – из 1 в 0, четвертый столбец – из 1 в 1.



а б

Рисунок 1 – Гистограмма частот переходов битовых значений: а – пустого контейнера, б – стеганоконтейнера

Для пустого контейнера и контейнера, содержащего встроенную информацию, число переходов в потоке НЗБ будет разным. Распределение НЗБ стеганоконтейнера имеет, как правило, случайный характер. Соответственно число переходов в потоке НЗБ для всех состояний будет примерно одинаковым, что не свойственно пустому контейнеру (рис. 1 а, б) [13], [14].

Метод оценки частот появления *k*-битовых серий в потоке НЗБ элементов контейнера. Метод позволяет оценить равномерность распределения элементов в исследуемой последовательности на основе анализа частоты появления нулей и единиц, и серий, состоящих из k бит [15]. В битовом представлении исследуемой последовательности x подсчитывается, сколько раз встречаются нули и единицы ($k = 1$), серии-двойки (00, 01, 10, 11: $k = 2$), серии-тройки (000, 001, 010, 011, 100, 101, 110, 111: $k = 3$) и т.д. На основе результатов строится гистограмма.

Для JPEG-изображений гистограмма строится по значениям частот появления битовых серий в потоке НЗБ дискретных косинусных коэффициентов, отличных от –1, 0, 1.

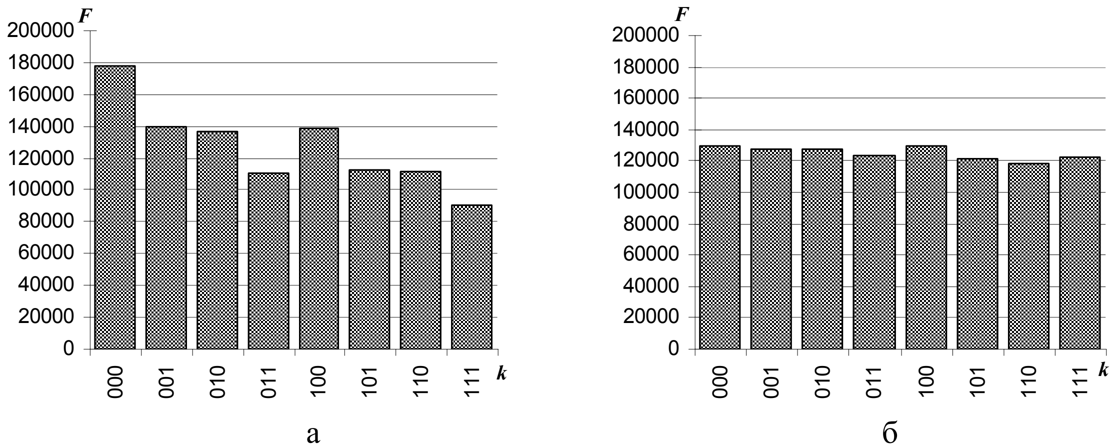


Рисунок 2 – Гистограмма частот серии-тройки ($k = 3$) в потоке НЗБ: а – пустого контейнера, б – стеганоконтейнера

Для незаполненных BMP и JPEG изображений не является характерным, чтобы значения частот всех компонентов находились достаточно близко (рис. 2 а). При внедрении информации значения частот сближаются (рис. 2 б). Этот факт используется при анализе.

Результаты работы метода зависят от стеганографического преобразования, используемого для встраивания скрываемых данных, а также от их объема. Как правило, выявление факта скрытия осуществимо при заполнении контейнера на 60% и выше.

Метод анализа распределения пар значений на основе критерия χ^2. В методе используется анализ гистограммы, полученной по элементам изображения и оценка распределения пар значений этой гистограммы [16]. Для BMP-файлов пары значений формируются значениями пикселов изображения, для JPEG – квантуемыми коэффициентами дискретного косинусного преобразования, которые отличаются по младшему биту. Младшие биты изображений не являются случайными. Частоты двух соседних элементов контейнера должны находиться достаточно далеко от значения частоты среднего арифметического этих элементов. В «пустом» изображении ситуация, когда частоты элементов со значениями $2N$ и $2N+1$ близки по значению, встречается достаточно редко. При встраивании информации данные частоты сближаются или становятся равными. Идея атаки хи-квадрат заключается в поиске этих близких значений и подсчете вероятности встраивания на основе того, как близко располагаются значения частот четных и нечетных элементов анализируемого контейнера. Особенностью алгоритма является последовательный анализ всего изображения и, соответственно, накапливание частот элементов.

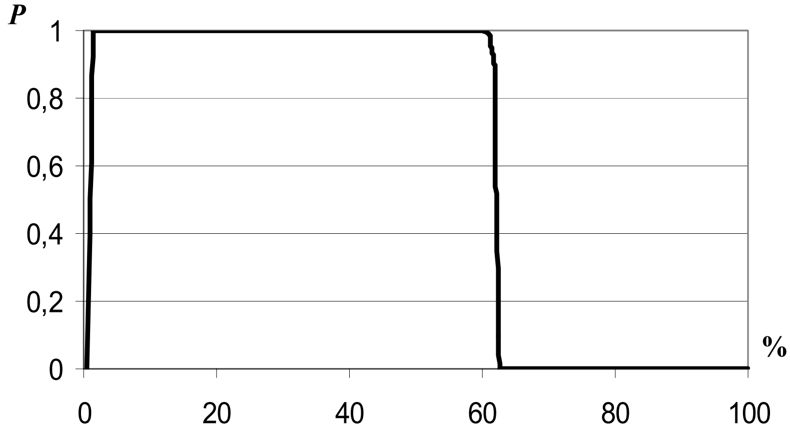


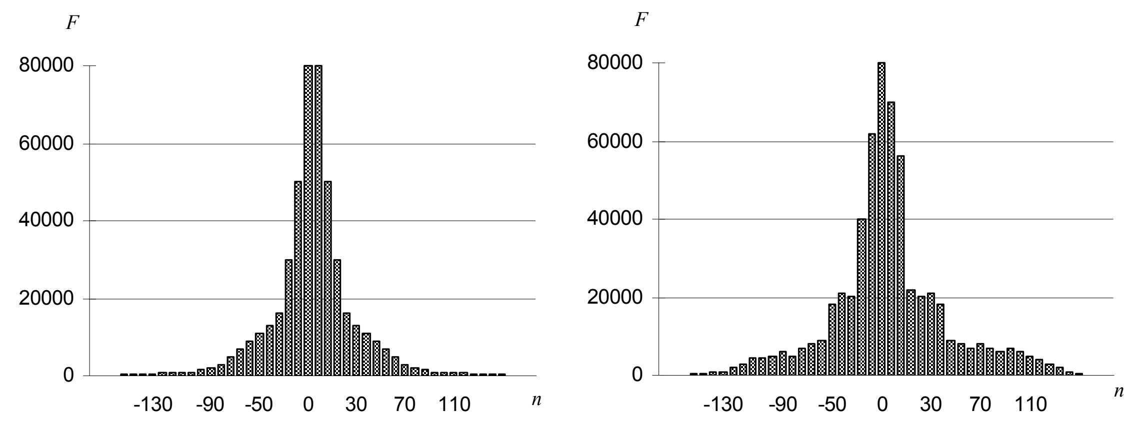
Рисунок 3 – Вероятность встраивания по критерию χ^2 при анализе стеганоконтейнера, полученного методом последовательной замены

Метод хи-квадрат является универсальным, так как подходит для анализа изображений, созданных различными программами скрытия. Однако результаты работы метода по критерию хи-квадрат в значительной мере зависят от способа скрытия данных. При последовательной записи в НЗБ элементов контейнера метод обеспечивает хорошие результаты (рис. 3), а при псевдослучайном выборе младших бит и рассеивании сообщения по всей длине контейнера метод не срабатывает. В работе [17] автор предложил совершенный «блочный» вариант данного метода. От классического метода он отличается тем, что анализируемое изображение разбивается на блоки определенного размера, которые могут как пересекаться, так и не пересекаться, и для каждого блока рассчитываются свои наборы частот элементов и свои вероятности скрытия. Кроме того, существует возможность выбора отдельных областей изображения для их последующего анализа. Такой подход позволяет выявлять наличие информации, скрытой псевдослучайным образом.

Метод анализа гистограмм, построенных по частотам элементов изображения. Метод позволяет оценить равномерность распределения элементов анализируемого изображения, а также определить частоту появления конкретного элемента.

Если разброс частот появления элементов в цветовых составляющих BMP-изображения стремится к нулю, то контейнер содержит скрытые данные. В противном случае контейнер считается пустым [15].

Для изображений в JPEG-формате строится гистограмма частот квантованных дискретных косинусных коэффициентов. Экспериментально обнаружено, что огибающая гистограммы пустого изображения имеет более гладкий характер (рис. 4 а) по сравнению с гистограммами изображений, содержащими стеганографическое вложение (рис. 4 б). Конечно, в зависимости от характера и степени сжатия изображения, гистограммы могут изменяться – в них могут появляться скачки и провалы, но важно то, что скрытие информации меняет общий вид гистограмм. Большинство стеганографических программ, работающих с JPEG, скрывают данные в младшие биты дискретных коэффициентов, отличных от 0 и 1. Как следствие, частоты 0-х и 1-х DCT не изменяются, в то время как все остальные частоты либо уменьшаются, либо увеличиваются в зависимости от алгоритма встраивания. При значительных объемах скрываемой информации гистограммы часто приобретают ступенчатый характер, что нетипично для обычных JPEG-изображений [17].

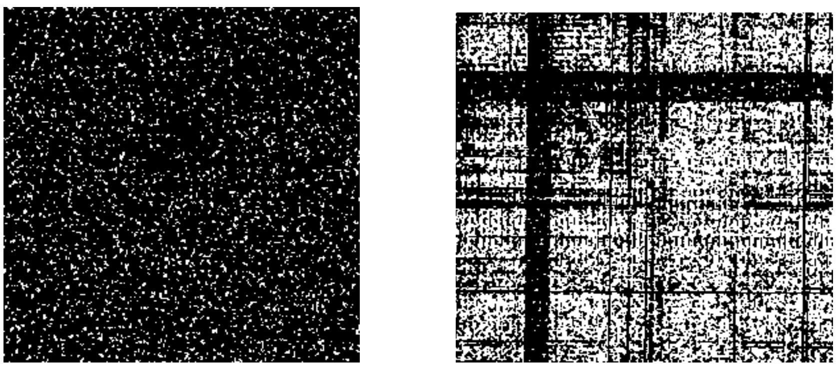


а б

Рисунок 4 – Гистограмма частот дискретных косинусных коэффициентов: а – исходного изображения, б – изображения, содержащего скрытую информацию

Метод анализа распределения элементов изображения на плоскости. Метод предназначен для определения зависимостей между элементами исследуемой последовательности.

На плоскость (поле) размером $(2^R-1)\times(2^R-1)$, где R – разрядность элемента последовательности, наносятся точки с координатами (x_i, x_{i+1}), x_i – элементы исследуемой последовательности x, $i=1,2,...,n-1$, n – длина последовательности. По полученной «картине» проводится анализ.



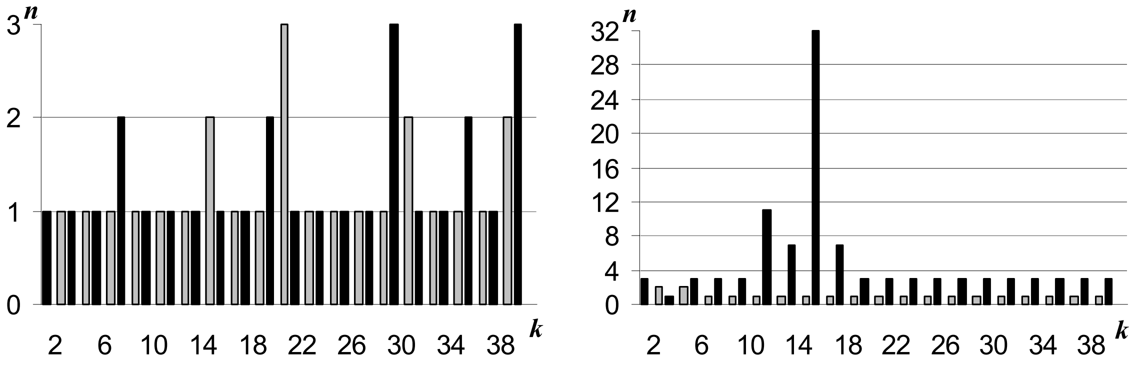
а б

Рисунок 5 – Распределение на плоскости элементов: а – изображения, содержащего скрытую информацию, б – исходного изображения

Если точки по всему полю расположены хаотично, то между элементами последовательности отсутствуют зависимости, что характерно для контейнеров со встроенными данными (рис. 5 а). В случае незаполненного контейнера точки на поле будут расположены неравномерно или образовывать «узоры» (рис. 5 б) [15].

Метод проверки распределения элементов на монотонность. Метод позволяет оценить равномерность распределения элементов изображения по результатам анализа длин участков невозрастания и неубывания элементов последовательности.

Исследуемая последовательность x графически представляется в виде следующих друг за другом непересекающихся участков невозрастания и неубывания элементов последовательности.



а б

Рисунок 6 – Проверка на монотонность: а – изображения, содержащего скрытую информацию, б – исходного изображения

Так как статистические свойства стеганоконтейнера близки к свойствам случайной последовательности, то вероятность появления участка невозрастания (неубывания) будет тем меньше, чем больше его длина n [15].

Статистические методы не являются средством, позволяющим со 100%-й надежностью определять наличие скрытой информации. Они дают возможность аналитику с определенной вероятностью судить о том, используется стеганография или нет.

Помимо приведенных выше, существует еще ряд методов, основанных на различных математических моделях процесса стеганографии [18], [19]. Анализ показал, что в настоящее время существует определенное отставание в развитии методов стеганоанализа от методов стеганопреобразования. Таким образом, практическая стойкость стеганосистем напрямую зависит от развития стеганоаналитических методов.

Рассмотренные методы могут применяться в виде отдельного инструментария, используемого стеганоаналитиком или в виде модулей в составе сложных стеганографических систем анализа для обеспечения проверки графической информации в автоматическом режиме. Автоматизация процесса стеганоанализа позволит выделять на множестве результатов те из них, которые способствуют минимизации вероятности ошибки второго рода при заданном уровне вероятности ошибки первого рода, обеспечить наглядность результатов анализа.

Описанные методы анализа предлагается применять к потенциальному контейнеру последовательно. Они представлены в порядке убывания степени доверия положительным результатам их применения (скрытая информация обнаружена), полученным опытным путем. При получении положительного ответа в результате работы очередного метода анализ следует остановить, а анализируемый контейнер считать носителем информации, скрытой с использованием стеганографических методов. В случае отсутствия положительного ответа после применения всех перечисленных методов анализируемый контейнер следует считать пустым.

Стеганоанализ потенциального контейнера в условиях многократных срабатываний статистических методов при условии несрабатывания сигнатурных и схемных методов носит условный характер. При использовании исключительно статистических методов необходимо длительное наблюдение за стеганоканалом и значительные усилия опытного аналитика. Кроме того, необходимо знание алгоритма стеганопреобразования. Необходимым условием для установления факта присутствия в контейнере скрытой информации является срабатывание сигнатурных или схемных методов.

Выводы

Представленный набор методов направлен на выявление наличия данных, скрытых в графических файлах форматов BMP и JPEG. Комплексное применение различных методов стеганоанализа даст возможность гибко подходить к вопросу о возможном существовании скрытно встроенной информации, свести к минимуму вероятности ошибок первого и второго рода при обнаружении стеганографического скрытия информации. Оба вида ошибок отражают надежность и достоверность результатов анализа. Если минимизация вероятности ошибки первого рода сказывается только на уменьшении загруженности системы стеганоанализа за счет снижения числа постобработок, то вероятность ошибки второго рода отвечает за эффективность применяемого стеганоаналитического метода.

Литература

1. Задірака В.К. Комп’ютерна криптологія : підручник / В.К. Задірака, О.С. Олексюк. – Київ, 2002. – 504 с.
2. E. Adelson. Digital Signal Encoding and Decoding Apparatus. – U.S. Patent. – No. 4,939515 (1990).
3. Cachin C. An Information-Theoretic Model for Steganography / C. Cachin // Proceeding of 2nd Workshop of Information Hiding. – USA, 1998. – May, 13. – 12 p.
4. Разинков Е.В. Стойкость стеганографических систем / Е.В. Разинков, Р.Х. Латыпов // Учёные записки Казан. гос. ун-та. – Казань, 2009. – Т. 151, № 2. – С. 126-132.
5. Гизунов Д.С. Методика автоматизированного обнаружения скрытой информации в компьютерных файлах / Д.С. Гизунов, О.А. Демченко, Е.И. Никутин // Известия ТРТУ. – 2006. – Т. 71, № 16. – С. 49-53.
6. Provos N. Detecting steganographic content on the internet / N. Provos, P. Honeyman. // Technical Report CITI 01-1a, University of Michigan, 2001.
7. Girod B. The information theoretical significance of spatial and temporal masking in video signals / B. Girod Proc. of the SPIE Human Vision, Visual Processing, and Digital Display. – 1989. – Vol. 1077. – P. 178-187.
8. Алиев А.Т. Оценка стойкости систем скрытой передачи информации / А.Т. Алиев, А.В. Балакин // Известия ТРТУ. Тематический выпуск. Материалы VII Международной научно-практической конференции «Информационная безопасность». – Таганрог : Изд-во ТРТУ, 2005. – № 4 (48). – С. 199-204.
9. Алиев А.Т. О применении стеганографического метода LSB к графическим файлам с большими областями монотонной заливки / А.Т. Алиев // Вестник ДГТУ. – Ростов-на-Дону, 2004. – Т. 4, № 4 (22). – С. 454-460.
10. Швидченко И.В. Анализ криптостеганографических алгоритмов / И.В. Швидченко // Проблемы управления и информатики. – 2007. – № 4. – С. 149-155.
11. Грибунин В.Г. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – М. : Солон-Пресс, 2002. – 272 с.
12. Барсуков В.С. Оценка уровня скрытности мультимедийных стеганографических каналов хранения и передачи информации / В.С. Барсуков, А.П. Романцов // Специальная Техника. – 2000. – № 1.
13. Кустов В.Н., Параскевопуло А.Ю. Простые тайны стегоанализа / В.Н. Кустов, А.Ю. Параскевопуло // Защита информации, INSIDE. – 2005. – № 4. – С. 72-78.
14. Голуб В.А. Комплексный подход для выявления стеганографического скрытия в JPEG-файлах / В.А. Голуб, М.А. Дрюченко // Инфокоммуникационные технологии. – 2009. – Т. 7, № 1. – С. 44-50.
15. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М. : КУДИЦ-ОБРАЗ, 2003.
16. Westfeld A. Attacks on Steganographic Systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos and S-Tools-and Some Lessons Learned / A. Westfeld, A. Pfitzmann // 3rd International Workshop on Information Hiding (2000).
17. Дрюченко М.А. Алгоритмы выявления стеганографического скрытия информации в jpeg-файлах / М.А. Дрюченко // Вест. Воронеж. гос. ун. Системный анализ и информационные технологии. – 2007. – № 1. – С. 21-30.
18. Fridrich J. Steganalysis of JPEG Images: breaking the / J. Fridrich, M. Goljan, D. Hogea // F5 algorithm, 5th Information Hiding Workshop, Noordwijkerhout, The Netherlands, 7 – 9 October 2002. – Режим доступа : http://www.ws.binghamton. edu/fridrich/Research/f5.pdf
19. Fridrich J. Reliable Detection of LSB steganography in grayscale and color images / J. Fridrich, M. Goljan, R. Du // Proc. of the ACM, Special Session on Multimedia Security and Watermarking. – Ottawa, Canada, October 5, 2001. – P. 27-30.

І.В. Швідченко

Методи стеганоаналізу для графічних файлів

Стаття присвячена проблемі виявлення стеганографічного приховання у файлах форматів BMP і JPEG. Проводиться аналіз різних стеганоаналітичних методів. Приводиться їх класифікація і короткий огляд. Для встановлення факту присутності в контейнері прихованої інформації пропонується послідовне застосування представлених методів.

I.V. Shvidchenko

Steganoanalysis Methods for Graphic Files

The article is devoted to a problem of detection of steganographic hiding in files of BMP and JPEG formats. The analysis of various steganoanalytical methods is carried out. Their classification and brief review is presented. The consecutive application of presented methods is offered to establish the fact of the hidden information presence in container.

Статья поступила в редакцию 30.06.2010.